



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/623,112

07/18/2003

Gary G. Liu

10664-166001

4468

26181 7590 05/27/2008

FISH & RICHARDSON P.C.

PO BOX 1022

MINNEAPOLIS, MN 55440-1022

EXAMINER

LI, GUANG W

ART UNIT

PAPER NUMBER

2146

MAIL DATE

DELIVERY MODE

05/27/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/623,112	<b>Applicant(s)</b> LIU, GARY G.	
	<b>Examiner</b> Guang Li	<b>Art Unit</b> 2146	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 28 February 2008.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-23, 28-52 and 56-58 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-23, 28-52 and 56-58 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |                                                                                      |                                                                   |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____                                                          | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 02/28/2008 has been entered.
2. It is hereby acknowledged that the following papers have been received and placed of record in the file: Amendment date 02/28/2008
3. Claims 1-23, 28-52 and 56-58 are presented for examination.

### ***Response to Arguments***

4. Applicant's arguments filed 02/28/2008 have been fully considered but they are not persuasive. The examiner maintains his rejection that Pickup references still teaches limitations in claims 8-12 and 20-23.
5. Applicant's argues the reference of Pickup does not teaches the following limitations:

- Pickup des not teaches or suggest using the individual list to check whether a sender is included in a list of confirmed senders associated with any other spam filter in the network (Recipient whitelist sender as local stored list of confirmed senders "Recipient whitelist sender" Pickup:Fig.1 diamond box Recipient whitelist sender and (After checking the recipient white list senders then go back to check the System-wide white sender list where all the recipients share authorizes list of users see Fig.1).

- Pickup's recipients do not verify a sender message with Pickup's mail server (request for verification to the sender of an unauthorized email "verification means operating, upon detection of an unauthorised electronic mail, to send a request for verification to the sender of an unauthorised electronic mail" see Pickup: ¶[0045])

6. Applicant's arguments with respect to claims 1-7, 13-19, 28-52 and 56-58 have been considered but are moot in view of the new ground(s) of rejection.

**Oath/Declaration**

7. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63**.

***Claim Rejections - 35 USC § 102***

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 8-12 and 20-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Pickup (US 2003/01212791 A1).

10. Regarding claim 8, Pickup teaches a method for identifying a spam message comprising:

receiving a message at a spam filter in a network that includes a plurality of spam filters, each spam filter having an associated list of confirmed senders (share the same

list of authorized senders in each recipient "there are a plurality of recipients, and each recipient has a list of authorised senders. In an alternative form to this, a plurality of recipients share the same list of authorised senders" see¶[0016]);

Identifying the sender of the message (check the message after receiving message see Fig.1) ;

determining if the sender has been previously confirmed as a confirmed sender including:

determining, using a locally stored list of confirmed senders (Recipient whitelist sender as local stored list of confirmed senders "Recipient whitelist sender"

Pickup:Fig.1 diamond box Recipient whitelist sender), if the sender is includes a list of confirmed senders associated with any other spam filter in the network (After checking the recipient white list senders then go back to check the System-wide white sender list where all the recipients share authorizes list of users see Fig.1); and

if so, forwarding the received message to a recipient without separately confirming the sender in each spam filter (If the sender in the system-wide whitelist sender or recipient whitelist sender, the message will deliver email to recipient see Pickup: Fig.1).

11. Regarding claim 9, Pickup teaches the method of claim 8 wherein the messaging system is an email system (system for authorizing electronic mail see Pickup: ¶[0001]).

12. Regarding claim 10, Pickup teaches the method of claim 8 further comprising sharing the locally stored list of confirmed senders associated with another spam filter (the recipient whitelist senders and with system wide-white list sender shared the same

authorized senders "In an alternative form to this, a plurality of recipients share the same list of authorised senders" see Pickup: Fig.1).

13. Regarding claim 11, Pickup teaches the method of claim 8, wherein if is determined that the sender has not been previously confirmed (a system for authorising electronic mail sent by an unauthorised sender to a recipient see ¶[0035]), the method further comprising:

    sending a confirmation to the sender (send a request for verification to the sender of an unauthorised email see ¶[0039]);

    verifying a response from the sender (wherein upon receipt of the verification from the sender see ¶[0040]); and

    if the response is acceptable, adding the sender to the locally stored list of confirmed senders (adding sender to recipient whitelist see Fig.1 and Fig.2 "the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient" see ¶[0040]) and sharing information with at least one other spam filter (shared authorized users with the system wide whitelist in the network see Fig.1) in the network, the information including information indicating that the sender has been confirmed (In an alternative form to this, a plurality of recipients share the same list of authorised senders" see¶[0016]).

14. Regarding claim 12, Pickup teaches the method of claim 11 wherein sharing information with at least one other spam filters includes publishing the locally stored list of confirmed senders at a central location that can be accessed by other spam filters

(system-wide whitelist that can be access from all the recipients see Pickup: Fig.1 System-wide whitelist sender).

15. Regarding claim 20, Pickup teaches a method for detecting spam in a messaging system comprising:

generating a list of confirmed message senders (updating a whitelist containing details of a recipient's authorised senders see Pickup: ¶[0026]) and maintaining the list (To automatically update the whitelist, the recipient can utilise the automatic updating mechanism see Pickup: ¶[0062]) at a data center (the mail server is located outside of a network associated with the recipient see Pickup: ¶[0047]);

receiving a message at a spam filter in a network that includes a plurality of spam filters(share the same list of authorized senders in each recipient "there are a plurality of recipients, and each recipient has a list of authorised senders. In an alternative form to this, a plurality of recipients share the same list of authorised senders" see Pickup: ¶[0016]);

verifying with the data center (request for verification to the sender of an unauthorized email "verification means operating, upon detection of an unauthorised electronic mail, to send a request for verification to the sender of an unauthorised electronic mail" see Pickup: ¶[0045]) by the spam filter (Spam filter identifying unauthorized mail and request for verification "identification means for identifying unauthorised electronic mail sent to the recipient by reference to the whitelist" see Pickup: ¶[0044]) that the sender of the message is a confirmed message sender (system-wide whitelist sender and global whitelist see Pickup: ¶[0064]), and

if it is determined that the sender is a confirmed message sender, forwarding the received message to a recipient without separately confirming the sender (the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see Pickup: ¶[0040]).

16. Regarding claim 21, claim 21 is rejected for the same reason in claim 2 as set forth hereinabove.

17. Regarding claim 22, Pickup teaches the method of claim 20 further comprising sharing the list with at least two spam filters in the network (two or more recipients share the same list "there are a plurality of recipients, and each recipient has a list of authorised senders. In an alternative form to this, a plurality of recipients share the same list of authorised senders" see ¶[0016]).

18. Regarding claim 23, Pickup teaches the method of claim 20 wherein if it is determined that the sender is not a confirmed message sender (system for authorizing electronic mail sent by an unauthorized sender to a recipient see ¶[0035]), the method further comprising:

sending, from the data center, a confirmation to the sender (forwarding a request for verification to the sender see ¶[0025]); verifying a response received at the data center from the sender (verification means operating, upon detection of an unauthorized email, to send a request for verification to the sender of an authorized email see ¶[0039])

if the response is acceptable, adding to the list of confirmed message senders a name associated with the sender (wherein upon receipt of the verification from the



sender, the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]); and sharing information including the name with other spam filters in the network (a plurality of recipients share the same list of authorised senders see¶[0016]).

### ***Claim Rejections - 35 USC § 103***

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

20. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

21. Claims 1-7, 13-14, 33-44, 50-52 and 56-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup (US 2003/0212791 A1) in view of Rounthwaite et al. (US 7,219,148).

22. Regarding claim 1, Pickup teaches a method for detecting spam in a messaging system (a method of authorising electronic mail that utilises a recipient's list of authorised senders see abstract) comprising:

generating a white list of confirmed message senders (updating a whitelist containing details of a recipient's authorised senders see ¶[0026]), each of said confirmed message senders being authorized to send messages as evidenced by prior receipt of a response to a confirmation message ("the sender is added to the list of authorised senders and the electronic mail is forwarded to the recipient" see ¶[0011]);

using the white list at a given one of the plurality of spam filters to determine if a sender of a received message has been previously confirmed ("the request for verification sent to the recipient can be forwarded only if received within a predetermined time of the recipient sending a message to the sender. This will allow the recipient to "match" requests for verification with emails that they have previously sent" see ¶[0021]); and

forwarding the received message to a recipient without separately confirming the sender if it is determined that the sender has been previously confirmed ("Where verification is received, the sender is added to the recipient's whitelist and further emails from the sender can be delivered to the recipient without the requirement for a verification step" see ¶[0063]).

Pickup does not explicitly disclose distributing the white list among a plurality of spam filters in the messaging system.

Rounthwaite teaches distributing the white list among a plurality of spam filters in the messaging system (distribute the new filter to individual email clients "The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating Internet service providers (ISP), to the email or message servers, to

individual email clients, to an update server, and/or to the central databases of individual companies" see Rounthwaite: col.9 lines 7-11). Rounthwaite further provides the advantage of Users which are identified as spam-fighter are asked to vote on whether a selection of their incoming email messages is individually either legitimate mail or junk mail (see Abstract).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup and Rounthwaite before them at the time the invention was made to modify the method for detecting spam in a messaging system of Pickup to include (or to use, etc.) distributing the white list among a plurality of spam filters in the messaging system as taught by Rounthwaite.

One of ordinary skill in the art would have been motivated to make this modification in order to update the spam filters for maintain purpose in view of Rounthwaite.

23. Regarding claim 2, Pickup together with Rounthwaite taught the method for detecting spam according to claim 1, as described above. Pickup further teaches wherein the messaging system is an email system (system for authorizing electronic mail see Pickup: ¶[0001]).

24. Regarding claim 3, Pickup together with Rounthwaite taught the method for detecting spam according to claim 1, as described above. Rounthwaite further teaches wherein distributing the white list includes distributing the white list with at least two spam filters (distribute the new filter to individual email clients "The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating

internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies” see Rounthwaite: col.9 lines 7-11).

25. Regarding claim 4, Pickup together with Rounthwaite taught the method for detecting spam according to claim 1, as described above. Pickup further teaches wherein if the sender has not been previously confirmed (a system for authorising electronic mail sent by an unauthorised sender to a recipient see Pickup: ¶¶[0035]), the method further includes:

- sending a confirmation to the sender (send a request for verification to the sender of an unauthorised email see Pickup: ¶¶[0039]);

- verifying a response from the sender (wherein upon receipt of the verification from the sender see Pickup: ¶¶[0040]); and

- if the response is verified, adding the sender to the white list at the given spam filter (the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see Pickup: ¶¶[0040]) and sharing the information associated with the added sender with other spam filters in the messaging system (In an alternative form to this, a plurality of recipients share the same list of authorised senders” see Pickup: ¶[0016]).

26. Regarding claim 5, Pickup together with Rounthwaite taught the method for detecting spam according to claim 1, as described above. Rounthwaite further teaches wherein distributing includes publishing the white list at a central location (filter distributed to a central database “The new filter 116 can be distributed on an ongoing

basis by a distribution component 118 across participating internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies” see Rounthwaite: col.9 lines 7-11).

27. Regarding claim 6, Pickup together with Rounthwaite taught the method for detecting spam according to claim 1, as described above. Rounthwaite further teaches further comprising maintaining the white list at a central location wherein using the white list includes checking the white list maintained at a central location (the whitelist at the server will be automatic update and share with other recipients “To automatically update the whitelist, the recipient can utilise the automatic updating mechanism of the present invention” see Pickup: ¶[0062]).

28. Regarding claim 7, Pickup together with Rounthwaite taught the method for detecting spam according to claim 1, as described above. Rounthwaite and Pickup further teach wherein the if the sender has not been previously confirmed, the method further comprising:

sending a confirmation to sender(send a request for verification to the sender of an unauthorised email see Pickup: ¶[0039]);

verifying a response from the sender(wherein upon receipt of the verification from the sender see Pickup: ¶[0040]); and

if the response is verified, adding the sender to the white list maintained at a central location (the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see Pickup: ¶[0040]) that is distributed

among the plurality of spam filters (distribute the new filter to individual email clients

"The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies" see Rounthwaite: col.9 lines 7-11).

29. Regarding claim 13, Pickup teaches a method for identifying a spam message comprising: receiving a message at a spam filter in a network that includes a plurality of spam filters, each spam filter having an associated list of confirmed senders; Identifying the sender of the message; determining if the sender has been previously confirmed as a confirmed sender including: determining, using a locally stored list of confirmed senders (Recipient whitelist sender as local stored list of confirmed senders "Recipient whitelist sender" Pickup:Fig.1 diamond box Recipient whitelist sender), if the sender is includes a list of confirmed senders associated with any other spam filter in the network (After checking the recipient white list senders then go back to check the System-wide white sender list where all the recipients share authorizes list of users see Fig.1); and if so, forwarding the received message to a recipient without separately confirming the sender in each spam filter (If the sender in the system-wide whitelist sender or recipient whitelist sender, the message will deliver email to recipient see Pickup: Fig.1). Pickup further teaches maintaining the locally stored list (Recipient white list see Pickup: Fig.1) of confirmed senders at a central location (the mail server is located outside of a network associated with the recipient see Pickup: ¶[0047]), and determining if the sender has been previously confirmed (the whitelist at the server will

be automatic update and share with other recipients “To automatically update the whitelist, the recipient can utilise the automatic updating mechanism of the present invention” see ¶[0062]).

Pickup does not explicitly disclose including checking other locally stored lists of confirmed senders associated with other spam filters at the central location.

Rounthwaite teaches including checking other locally stored lists of confirmed senders associated with other spam filters at the central location (new filter will be distributing over the network and use this new filter to all the other spam filters at the central location (system-wide list) “The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies” see Rounthwaite: col.9 lines 7-11).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup and Rounthwaite before them at the time the invention was made to modify the method for detecting spam in a messaging system of Pickup to include (or to use, etc.) including checking other locally stored lists of confirmed senders associated with other spam filters at the central location as taught by Rounthwaite.

One of ordinary skill in the art would have been motivated to make this modification in order to enhance spam filtering in view of Rounthwaite.

30. Regarding claim 14, Pickup together with Rounthwaite taught the method for detecting spam according to claim 8, as described above. Rounthwaite and Pickup

further teach wherein if the sender has not been previously confirmed, the method further comprising:

sending a confirmation to the sender (send a request for verification to the sender of an unauthorised email see Pickup: ¶[0039]);

verifying a response (wherein upon receipt of the verification from the sender see Pickup: ¶[0040]); and

if the response is acceptable, adding the sender to the locally stored list; and distributing the locally stored list among the plurality of spam filters (distribute the new filter to individual email clients "The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies" see Rounthwaite: col.9 lines 7-11).

31. Regarding claim 33, Pickup teaches a method for filtering spam in a messaging system (method of authorizing electronic mail sent by a sender to recipient see abstract) comprising:

confirming that a message sender can receive one or more messages (Send verification request back to sender block see fig.1);

using said information at a given one of the plurality of spam filters to determine if a message should be sent to an intended recipient without separately determining whether the message sender can receive one or more messages (wherein upon receipt



Art Unit: 2146

of the verification from the sender, the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[[0040]].

Pickup does not explicitly disclose distributing information indicating that the message sender can receive one or more messages among a plurality of spam filters in the messaging system.

Rounthwaite teaches distributing information indicating that the message sender can receive one or more messages among a plurality of spam filters in the messaging system (distribute the new filter to individual email clients and update individual spam filters/central database "The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies" see Rounthwaite: col.9 lines 7-11).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup and Rounthwaite before them at the time the invention was made to modify the method for detecting spam in a messaging system of Pickup to include (or to use, etc.) distributing information indicating that the message sender can receive one or more messages among a plurality of spam filters in the messaging system as taught by Rounthwaite.

One of ordinary skill in the art would have been motivated to make this modification in order to update the spam filters for maintain purpose in view of Rounthwaite.

32. Regarding claim 34, claim 34 is rejected for the same reason in claim 2 as set forth hereinabove.

33. Regarding claim 35, Pickup together with Rounthwaite taught the method for detecting spam according to claim 33, as described above. Pickup further comprising confirming at a first spam filter in the system that a sender of a message can receive messages ("verification means operating, upon detection of an unauthorized email, to send a request for verification to the sender of an authorized email" see Pickup: ¶[0039]).

34. Regarding claim 36, Pickup together with Rounthwaite taught the method for detecting spam according to claim 35, as described above. Pickup further comprising receiving the message at a second spam filter (Electronic message received at the first system-wide filters (Whitelist and blacklist) and process to recipient filters (whitelist and blacklist see Pickup: Fig.1).

35. Regarding claim 37, Pickup together with Rounthwaite taught the method for detecting spam according to claim 33, as described above. Rounthwaite further teaches distributing information developed by the first spam filter with one or more other spam filters in the messaging system (distribute the new filter to individual email clients "The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies" see Rounthwaite: col.9 lines 7-11).

36. Regarding claim 38, Pickup together with Rounthwaite taught the method for detecting spam according to claim 37, as described above. Pickup further comprising distributing the information with a data center (the mail server is located outside of a network associated with the recipient see Pickup: ¶[[0047]) and thereafter allowing access by each of the spam filters in the messaging system to the information (share the system-wide whitelist with all other recipients in the network see Pickup: ¶[[0016]).

37. Regarding claim 39, Pickup together with Rounthwaite taught the method for detecting spam according to claim 33, as described above. Pickup further teaches wherein the information is maintained in a list that includes one or more confirmed message senders ("there are a plurality of recipients, and each recipient has a list of authorised senders" see Pickup: ¶[[0016]).

38. Regarding claim 40, Pickup together with Rounthwaite taught the method for detecting spam according to claim 39, as described above. Rounthwaite further teaches wherein the list is distributed among with a plurality of the spam filters in the messaging system (distribute the new filters to individual email clients/central databases of individual companies "The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies" see Rounthwaite: col.9 lines 7-11).

39. Regarding claim 41, Pickup together with Rounthwaite taught the method for detecting spam according to claim 39, as described above. Pickup further teaches wherein the list (System-wide whitelist see Pickup: Fig.1) is maintained by a data

Art Unit: 2146

center (the mail server is located outside of a network associated with the recipient see Pickup: ¶[0047]) accessible by the spam filters in the messaging system (share the system-wide whitelist with all other recipients in the network see Pickup: ¶[0016]).

40. Regarding claim 42, Pickup together with Rounthwaite taught the method for detecting spam according to claim 41, as described above. Rounthwaite further teaches distributing the list with a plurality of spam filters in the messaging system (distribute the new filters to individual email clients/central databases of individual companies "The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies" see Rounthwaite: col.9 lines 7-11).

41. Regarding claim 43, Pickup together with Rounthwaite taught the method for detecting spam according to claim 37, as described above. Pickup further teaches maintaining a copy of the list at one or more of the of spam filters in the messaging system (list been keep update in the system-wide whitelist "continuously updating a list of authorized senders to filter unwanted electronic mail" see Pickup: ¶[0027]).

42. Regarding claim 44, Pickup together with Rounthwaite taught the method for detecting spam according to claim 37, as described above. Pickup further teaches associating a passcode with one or more of the confirmed senders in the list, and verifying a message received from a sender in the list including verifying the passcode specified by the sender (a non-machine readable code for sender verification

“utilise a request for verification where that request includes non-machine readable code to make it difficult for automated verification of the message” see Pickup: ¶¶0022}).

43. Regarding claim 50, Pickup teaches method for filtering spam, confirming that a message sender can receive one or more messages (Send verification request back to sender block see fig.1); sharing information indicating that the message sender can receive one or more messages among a plurality of spam filters in the messaging system (a plurality of recipients share the same list of authorised senders” see¶0016)). using said information at a given one of the plurality of spam filters to determine if a message should be sent to an intended recipient without separately determining whether the message sender can receive one or more messages. Pickup further teaches correlating sender-recipient data at a spam filter in the messaging system and determining a list of unacceptable senders using the sender-recipient data and the determined data (Blacklist see Fig.1); and sharing the list of unacceptable senders with other spam filters in the messaging system (sharing the whitelist and blacklist withal the recipient “a plurality of recipients share the same list of authorised senders” see¶0016)).

Rounthwaite teaches determining data related to how fast a list of recipients grows for a given sender (determining spammer based on the limitations “there may be limitations on the number of messages selected per user or per user per time period, or on the probability of selecting a message from any given user. Without such limits, a spammer could create an account” see col.6 lines 62-66).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup and Rounthwaite before them at the time the invention was made to

modify the method for filtering system of Pickup to include determining data related to how fast a list of recipients grows for a given sender as taught by Ref B.

One of ordinary skill in the art would have been motivated to make this modification in order to determining whether the senders is spammer or not based on the statistics in view of Rounthwaite.

44. Regarding claim 51, Pickup together with Rounthwaite taught the method for detecting spam according to claim 33, as described above. Pickup further teaches maintaining a list of recipients for each sender of messages processed by a given spam filter (each recipient has a whitelist and blacklists "each recipient has a list of authorised senders" See¶[0016]; Fig.1) .

45. Regarding claim 52, Pickup together with Rounthwaite taught the method for detecting spam according to claim 33, as described above. Pickup further teaches maintaining the list of recipients for each sender at a data center (the whitelist at the server will be automatic update and share with other recipients "To automatically update the whitelist, the recipient can utilise the automatic updating mechanism of the present invention" see ¶[0062]).

46. Regarding claim 56, Pickup teaches a method for minimizing spam in a messaging system, (a method of authorising electronic mail that utilises a recipient's list of authorised senders see abstract), the messaging system including a plurality of spam filters ("there are a plurality of recipients, and each recipient has a list of authorised senders. In an alternative form to this, a plurality of recipients share the same list of authorised senders" see¶[0016]), the method comprising:

receiving a request from one of the spam filters in the messaging system to verify if a sender of a message is a confirmed sender, a confirmed sender being a sender having a verified capability to receive messages; evaluating a list of confirmed senders (confirmation and verification of confirmed user "identifying an unauthorised electronic mail, the unauthorised electronic mail being addressed to the recipient and originating from a sender whose details are not included on the whitelist, forwarding a request for verification to the sender, receiving verification from the sender and including the sender's details on the whitelist" see ¶[0028-0030]);

if the sender is not included in the list of confirmed senders , confirming the sender including providing a notification to the sender (Send verification request back to the sender see Fig.1) and

upon receipt of a confirmation from the sender in response to the notification, including adding the sender to the list (forwarding a request for verification to the sender and receiving verification from the sender and including the sender's details on the whitelist see ¶[0025-0026]); and

notifying the one spam filter indicating whether the sender's status is confirmed (the plurality of recipients share the same list notify each other whether the sender is authorized user or not "there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this, a **plurality of recipients share the same list of authorised senders**" see ¶[0016]).

Pickup does not explicitly disclose distributing the sender's status with other spam filters in the messaging system.

Rounthwaite teaches distributing the sender's status with other spam filters in the messaging system (distribute the new filter to individual email clients "The new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet service providers (ISP), to the email or message servers, to individual email clients, to an update server, and/or to the central databases of individual companies" see Rounthwaite: col.9 lines 7-11). Rounthwaite further provides the advantage of Users which are identified as spam-fighter are asked to vote on whether a selection of their incoming email messages is individually either legitimate mail or junk mail (see Abstract).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup and Rounthwaite before them at the time the invention was made to modify the method for detecting spam in a messaging system of Pickup to include (or to use, etc.) distributing the sender's status with other spam filters in the messaging system as taught by Rounthwaite.

One of ordinary skill in the art would have been motivated to make this modification in order to update the spam filters for maintain purpose in view of Rounthwaite.

47. Regarding claim 57, Pickup together with Rounthwaite taught the method for detecting spam according to claim 56, as described above. Pickup further teaches wherein the step of confirming the sender is performed by a spam filter (Each recipient have individual whitelist and black list "each recipient has a list of authorised senders" see Pickup: ¶[0016]; Fig.1).



48. Regarding claim 58, Pickup together with Rounthwaite taught the method for detecting spam according to claim 56, as described above. Pickup further teaches wherein the step of confirming the sender is performed by the requesting spam filter (sender went through the inbound e-mail flowchart for filtering service and send verification message back to sender for confirmation see Pickup: Fig.1).

**49. Claims 45-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup (US 2003/0212791 A1) in view of Rounthwaite et al. (US 7,219,148) and further in view of Brown et al. (US 2004/0034694 A1).**

50. Regarding claim 45, Pickup together with Rounthwaite taught the method for filtering spam in a messaging system in claim 33. Pickup together with Rounthwaite teach confirming that message sender can receive one or more message, distributing information with other plurality of spam filters in the message system, using said distributing information to determined if a message should be send to intended recipient without separately confirmation ("the sender is added to the list of authorised senders and the electronic mail is forwarded to the recipient" see Pickup: ¶[0011]). Pickup further teaches wherein the information is maintained in a list that includes one or more confirmed message senders ("there are a plurality of recipients, and each recipient has a list of authorised senders" see Pickup: ¶[0016]) and associating a passcode with one or more of the confirmed senders in the list, and verifying a message received from a sender in the list including verifying the passcode specified by the sender (see Pickup: ¶[0022]).

Pickup together with Rounthwaite does not explicitly disclose prompting a sender in the list to enter a passcode upon an occurrence of an predefined event.

Brown teaches prompting a sender in the list to enter a passcode upon an occurrence of an predefined event (the process passes to block 808 which depicts the client email application prompting the sender to enter a passcode for the intended recipient see Brown: ¶[0053]). Brown further provides the advantage of recipient client email application, a determination is made regarding whether the passcode is included in the email (see abstract).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup through Brown before them at the time the invention was made to modify the method for filtering email system of Pickup and Rounthwaite to include prompting a sender in the list to enter a passcode upon an occurrence of an predefined event as taught by Brown.

One of ordinary skill in the art would have been motivated to make this modification in order to provide security purpose in view of Brown.

51. Regarding claim 46, Pickup through Brown taught the method for detecting spam according to claim 45, as described above. Brown further teaches detecting that an email address associated with the sender has been compromised, and prompting the sender to enter the passcode thereafter (the process passes to block 808 which depicts the client email application prompting the sender to enter a passcode for the intended recipient see Brown: ¶[0053]; Fig.8 blocks 806-808).

Art Unit: 2146

52. Regarding claim 47, Pickup through Brown taught the method for detecting spam as described above. Brown further teaches receiving a pass code from the confirmed message sender; and verifying the pass code is included in the message prior to forwarding the message from the confirmed message the sender to the intended recipient (sender's client email application inserting a passcode directive that includes the recipient's passcode as the first line in the body of the email message and transmitting the email to the intended recipient see Brown: ¶[0054], Fig.8 Blocks 810-812).

53. Regarding claim 48, Pickup through Brown taught the method for detecting spam according to claim 47, as described above. Brown further teaches automatically adding the passcode associated with the sender at a time for transmission of a message from the sender in the messaging system (when sender compose an email message, the passcode (save in sender address book see Brown: Fig.8 block 806) will added to the email and transmit email to intended recipient see Brown: Fig.8)

54. Regarding claim 49, Pickup through Brown taught the method for detecting spam according to claim 48, as described above. Brown further teaches providing a plug-in module for automatically adding the passcode, the plug-in module adapted to add the passcode prior to transmission to the messaging system (Features that added to adding the passcode to the normal email program that consider as plug in module see Brown: Fig.8 and Fig.10).

**55. Claims 15-19 and 28-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup (US 2003/0212791 A1) in view of Rounthwaite et al. (US 7,219,148) and further in view of Goldman et al. (US 2005/0021649 A1)**

56. Regarding claim 15, Pickup teaches a method for detecting a spammer in a network that includes a plurality of spam filters, the method comprising: collecting information relating from a plurality of the spam filter (identifying and intercepting an unauthorised electronic mail before delivery to the recipient, the unauthorised electronic mail being identified through a comparison of details of the sender with details contained on a list of authorised senders see Pickup: ¶[0009]).

Rounthwaite teaches determining a trend in the collected information; and identifying a spammer based on the trend (determining spammer based on the limitations "there may be limitations on the number of messages selected per user or per user per time period, or on the probability of selecting a message from any given user. Without such limits, a spammer could create an account" see Rounthwaite: col.6 lines 62-66).

Rounthwaite further provides the advantage of Users which are identified as spam-fighter are asked to vote on whether a selection of their incoming email messages is individually either legitimate mail or junk mail (see Abstract).

Pickup together with Rounthwaite does not explicitly disclose collecting information relating to a sender.

Goldman teaches collecting information relating to a sender (collecting outgoing message of the sender to determined whether is a spammer or not "If the sum total per

outgoing message exceeds some threshold amount, then that message and/or the respective sender can be flagged as a potential spammer" see Goldman: ¶¶[0011]).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup Through before them at the time the invention was made to modify the method and system for detecting spam of Pickup to include collecting information relating to a sender as taught by Goldman.

One of ordinary skill in the art would have been motivated to make this modification in order to improve spam-detecting system based on sender actions in view of Goldman.

57. Regarding claim 16, Pickup through Goldman taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches wherein collecting information includes collecting information relating to a number of messages sent by a sender to unrelated email addresses (there may be limitations on the number of messages selected per user" see col.6 lines 62-63).

58. Regarding claim 17, Pickup through Goldman taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches wherein determining trends includes correlating the messages received by an individual spam filter relating to a same sender (to detect as spammer based on the probability of selecting a message from any given user see Rounthwaite: col.6 lines 62-65).

59. Regarding claim 18, Pickup through Goldman taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches wherein identifying includes determining that a sender is a spammer if a number of messages

sent to unrelated email addresses exceeds a predetermined threshold (the disagreement vote all based on individual user action to vote whether the message is legitimate or spam “the number disagreements exceeds a threshold level, then the suspect users is consider untrustworthy” see Rounthwaite: col. 19 lines 54-56).

60. Regarding claim 19, Pickup through Goldman taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches wherein the threshold is time dependent (time period can be set in advance or the message can be held until receipt of a determined number of poll results similar to the message e.g. from the same IP address or with similar content see Rounthwaite: col.3 line 67 – col.4 lines 1-3).

61. Regarding claims 28-32, they are rejected for the same reason as claims 15-19. Pickup further teaches collecting information using data center (System-wide whitelist or Global whitelist that hosting in the network for identifying the sender permission see Pickup: ¶ [0064]).

### **Conclusion**

The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See **MPEP 707.05(c)**.

The following reference teaches execution of trial data.

- US 5,999,932 (Paul) teaches a system for eliminating unsolicited electronic mail generates and stores a user inclusion list including identification data for identifying e-mail desired by the user

- US 6,321,267 (Donaldson) teaches the system selectively accepts an electronic message sent from a sender through a remote host over a connection to a recipient at a server
- US 2003/0236847 A1 (Benowitz et al.) teach a method of authorizing communications includes receiving a communication from a sender
- US 2004/0210640 A1 (Chadwick et al.) teach email senders may transmit emails over the internet to a mail server that handles emails for a plurality of users (clients)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Guang Li whose telephone number is (571) 270-1897. The examiner can normally be reached on Monday-Friday 8:30AM-5:00PM(EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2146

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

May 23, 2008

GL

Patent Examiner

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2146